VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Cinthia Obladen de Almendra Freitas; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-156-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O VIII Encontro Virtual do CONPEDI, organizado pelo CONPEDI, teve como tema central "Direito Governança e Políticas de Inclusão". A partir dessa temática, foram promovidos intensos debates entre pesquisadores nacionais e internacionais, com apresentações de trabalhos previamente selecionados por meio de avaliação duplo-cega por pares.

Os artigos reunidos nesta publicação foram apresentados no Grupo de Trabalho "Direito, Governança e Novas Tecnologias II", realizado no dia 27 de junho de 2025, e refletem o estado atual das pesquisas desenvolvidas por graduandos e pós-graduandos em direito em diversas instituições brasileiras. O conjunto de trabalhos revela a diversidade temática e a profundidade das discussões jurídicas contemporâneas sobre os impactos da tecnologia na sociedade.

As apresentações cobriram uma ampla gama de tópicos que envolvem a interface entre tecnologia, direito, demonstrando um panorama das preocupações acadêmicas sobre o reconhecimento facial, a inteligência artificial e os desafios ao judiciário, direitos autorais e inteligência artificial, democracia digital e pós-verdade, governo digital, políticas públicas, sociedade digital e transformação do direito privacidade, desinformação e desigualdades digitais. Com o intuito de facilitar a leitura e destacar os enfoques abordados, os trabalhos foram organizados nos seguintes eixos temáticos:

1. Reconhecimento Facial, Vigilância e Direitos Fundamentais - Este eixo concentra estudos sobre o uso da tecnologia de reconhecimento facial no contexto da segurança pública e seus impactos sobre direitos fundamentais, com ênfase em discriminação algorítmica, proteção de

Reconhecimento facial para vigilância: comparação das aplicações da inteligência artificial em eventos de massa no Brasil e em experiências internacionais (Yuri Nathan da Costa Lannes / Júlia Mesquita Ferreira / Lais Faleiros Furuya)

Reconhecimento facial e a violação de direitos fundamentais: discriminação algorítmica, vigilância em massa e a necessidade de regulação no Brasil (Bibiana Paschoalino Barbosa / Anderson Akira Yamaguchi / Ruan Ricardo Bernardo Teodoro)

2. Inteligência Artificial, Judiciário e Regulação - Este eixo analisa a aplicação da inteligência artificial no sistema de justiça e os desafios regulatórios do contexto brasileiro, com foco na governança tecnológica e nos riscos da opacidade algorítmica:

O uso da inteligência artificial no Poder Judiciário brasileiro e a Resolução do Conselho Nacional de Justiça n.º 615/2025 (Simone Stabel Daudt / Rosane Leal Da Silva / Julia Daudt Mansilha)

Inteligência artificial e a crise da regulação clássica: um estudo sobre o atual contexto regulatório brasileiro (Fernanda Sathler Rocha Franco / Luiz Felipe de Freitas Cordeiro / Marina Moretzsohn Chust Trajano)

Direito à transparência, inteligência artificial e desafios técnicos: uma análise do Projeto de Lei nº 2.338/23 (Fernanda Sathler Rocha Franco)

Opacidade algorítmica estratégica e risco sistêmico informacional nas eleições: considerações para uma governança anti-manipulação das democracias digitais (Helena Dominguez Paes Landim Bianchi / Maria Clara Giassetti Medeiros Corradini Lopes)

3. Direitos Autorais, Propriedade Intelectual e IA - Reúne pesquisas que discutem a

O uso indevido das imagens geradas pelos filtros Ghibli e a proteção do direito à imagem sob a perspectiva da Lei Geral de Proteção de Dados (LGPD) (Lilian Benchimol Ferreira / Maria Cristina Almeida Pinheiro de Lemos / Narliane Alves De Souza E Sousa)

4. Democracia Digital, Desinformação e Pós-Verdade - Trabalhos que discutem os impactos da tecnologia na propagação de fake news, movimentos ideológicos e desinformação em contextos democráticos:

Movimentos antifeministas e desinformação: quando a misoginia se propaga em fake News (Juliana Aparecida de Jesus Pires / Irineu Francisco Barreto Junior / Samyra Haydêe Dal Farra Naspolini)

A sociedade do cansaço e pós-verdade: fake news sobre as urnas eletrônicas (Bruna Figueiredo Dos Santos / Zulmar Antonio Fachin)

5. Governança Digital, Políticas Públicas e Compartilhamento de Dados - Aborda o papel das políticas públicas e da governança digital no século XXI, destacando os desafios do uso de dados por entes públicos e o potencial das tecnologias no desenvolvimento social:

Governança digital e democracia no século XXI: o papel das políticas públicas na era da inteligência artificial (Daniel David Guimarães Freire)

O potencial do compartilhamento de dados entre entes federativos para o desenvolvimento de políticas públicas inteligentes (Ana Cristina Neves Valotto Postal / Paulo Cezar Dias / Rodrigo Abolis Bastos)

6. Tecnologia, Sustentabilidade e Transformação Econômica - Esse eixo reúne trabalhos sobre o impacto das inovações tecnológicas em setores como o agronegócio e as ecotecnologias, destacando aspectos de compliance, sustentabilidade e tributação:

7. Sociedade Digital, Infância e Transformações do Direito - Trabalhos que discutem os efeitos das tecnologias emergentes sobre a infância, os registros civis, a exposição digital e os reflexos no Direito Civil e registral:

A vitrine digital da infância e o papel do Direito: análise do sharenting e das iniciativas legislativas brasileiras (Ana Júlia Oliveira Machado / Bibiana Paschoalino Barbosa)

Inovações e desafios na implantação das tecnologias notariais e registrais: uma análise do e-Notariado cinco anos após sua criação (José Luiz de Moura Faleiros Júnior / Francislene Silva Da Costa Garcia / Isabela da Cunha Machado Resende)

O impacto da tecnologia na sociedade aberta: desafios e oportunidades para o Direito Civil (Viviane Ferreira Mundim / Najua Samir Asad Ghani / Patricia Maria Paes de Barros)

Treinamento de inteligência artificial e consumidores mudando marcas de seus bens em protesto político (Carlos Alberto Rohrmann)

Espera-se que esta publicação contribua para o aprofundamento dos debates sobre os desafios jurídicos da era digital, estimulando novas reflexões e a produção científica crítica e inovadora. Agradecemos a todos os pesquisadores, pareceristas e organizadores que tornaram este Grupo de Trabalho possível. Desejamos uma excelente leitura!

Cinthia Obladen de Almendra Freitas – PUC-PR

Liton Lanes Pilau Sobrinho – UNIVALI

Yuri Nathan da costa Lannes - FDF

A TECNOLOGIA DE RECONHECIMENTO FACIAL FRENTE AOS DIREITOS DAS CRIANÇAS E ADOLESCENTES: UMA ANÁLISE DOS RISCOS NO CONTEXTO DIGITAL

FACIAL RECOGNITION TECHNOLOGY; CHILDREN AND ADOLESCENTS; DATA PROTECTION; DIGITAL PRIVACY; CLASSIFICATION OF THE 4CS.

Aline Martins Rospa
Rosane Leal Da Silva

Resumo

As tecnologias de reconhecimento facial (TRFs) estão se tornando cada vez mais presentes na sociedade contemporânea, trazendo desafios relevantes, sobretudo quando aplicadas ao público infantojuvenil. Este estudo analisa os riscos da coleta indiscriminada de dados de crianças e adolescentes por empresas de tecnologia, destacando possíveis violações de seus direitos fundamentais. O objetivo central é compreender as implicações legais dessa coleta no contexto da proteção de dados pessoais. A pesquisa é qualitativa, com método monográfico e técnicas de análise documental e bibliográfica, examinando legislações nacionais e internacionais, além de relatórios especializados. Os resultados indicam que o uso crescente das TRFs expõe os jovens a riscos como a violação da privacidade e a coleta indevida de dados. A classificação dos 4Cs (Conteúdo, Contato, Conduta e Contrato) é empregada como ferramenta para compreender esses riscos e propor medidas de mitigação. Embora existam projetos de lei em trâmite no Brasil que tratam da questão, ainda há lacunas regulatórias significativas, agravadas pela opacidade com que muitas empresas lidam com os dados coletados. Um exemplo é o TikTok, que prevê em seus termos de uso a coleta de dados biométricos em determinadas jurisdições. Assim, o estudo destaca a urgência da criação de normas específicas para o uso das TRFs, defendendo uma abordagem que garanta a proteção integral e o protagonismo digital de crianças e adolescentes. Enfatiza-se a importância da atuação conjunta do Estado, da sociedade e da família na proteção da privacidade e da dignidade infantojuvenil no ambiente digital.

international legislation and specialized reports. The findings reveal that the growing use of FRTs exposes young people to risks such as privacy violations and improper data collection. The 4Cs classification (Content, Contact, Conduct, and Contract) is used as a framework to understand these risks and propose mitigation strategies. Although there are ongoing legislative initiatives in Brazil addressing this issue, significant regulatory gaps remain, worsened by the lack of transparency from companies regarding how collected data is processed. An example is TikTok, whose terms of use include the collection of biometric data in certain jurisdictions. Therefore, the study highlights the urgent need for specific regulations concerning FRTs, advocating for an approach that ensures comprehensive protection and promotes digital agency for children and adolescents. It emphasizes the importance of coordinated efforts among the State, society, and families to safeguard minors' privacy and dignity in the digital environment.

Keywords/Palabras-claves/Mots-clés: Facial recognition technology, Children and adolescents, Data protection, Digital privacy, 4cs classification

INTRODUÇÃO

As tecnologias de reconhecimento facial (TRFs) são cada vez mais utilizadas em diversas áreas, desde a segurança pública, autorização de transações financeiras, controle de acesso em aeroportos e áreas de alta segurança, desbloqueio de smartphones e notebooks, e monitoramento de pacientes em hospitais.

O uso crescente das TRFs por crianças e adolescentes têm moldado a forma como esses sujeitos interagem, aprendem e se desenvolvem. No Brasil, essa tendência é especialmente evidente, com plataformas digitais ocupando um espaço central no cotidiano das pessoas dessa faixa etária. Por um lado, essas tecnologias oferecem oportunidades para o aprendizado, a socialização e o desenvolvimento pessoal, mas, por outro, apresentam riscos substanciais, especialmente no que tange à privacidade e à segurança. Entre esses riscos, destaca-se a coleta de dados sensíveis, como os de reconhecimento facial, por empresas de tecnologia, o que traz preocupações éticas, sociais e legais.

O reconhecimento facial, uma das aplicações da inteligência artificial que mais se desenvolveu nos últimos anos, está cada vez mais presente em dispositivos e plataformas acessadas por menores de idade. No entanto, a coleta e o uso desses dados podem comprometer os direitos fundamentais das crianças e adolescentes, expondo-os a violações de privacidade, discriminação algorítmica e outros impactos negativos decorrentes da formação de perfis automatizados. Nesse cenário, surge a necessidade de uma análise crítica sobre como as empresas de tecnologia utilizam essas informações e como a legislação vigente aborda tais práticas.

Embora existam normas legais para a proteção de dados pessoais no Brasil, como a Lei Geral de Proteção de Dados (LGPD), essas regulamentações ainda carecem de mecanismos específicos que tratem da coleta e do uso de dados de reconhecimento facial de crianças e adolescentes. Para analisar esse contexto, foi utilizada no estudo a classificação dos riscos online baseada nos "4Cs" cujas iniciais referem-se aos riscos de conteúdo, contato, conduta e contrato que surgem da exposição digital das crianças e adolescentes (Livingstone; Stoilova, 2021). Contudo, se faz necessário adaptar essa teoria às peculiaridades das tecnologias de reconhecimento facial (TRFs) e suas implicações específicas para a infância e a adolescência.

Assim sendo, esse estudo foi provocado pelo seguinte problema de pesquisa: quais são os principais riscos associados à coleta de dados de reconhecimento facial de crianças e adolescentes por empresas de tecnologia? O objetivo geral é analisar os riscos associados à coleta de dados de reconhecimento facial de crianças e adolescentes, avaliando suas implicações legais no contexto do direito à proteção de dados pessoais.

A pesquisa adotará uma abordagem qualitativa, com foco na análise dos riscos presentes na coleta de dados de reconhecimento facial de crianças e adolescentes pelas empresas de tecnologia no ambiente digital. O método de procedimento será o monográfico, pois possibilita um estudo aprofundado dos aspectos legais, éticos e sociais envolvidos, considerando os impactos das tecnologias digitais na infância e adolescência no que tange a coleta dos seus dados de

reconhecimento facial. A pesquisa utilizará duas técnicas principais: a pesquisa documental, que envolverá a análise de legislação brasileira, tratados internacionais e convenções sobre os direitos da criança e do adolescente; e a pesquisa bibliográfica, com uma revisão abrangente da literatura existente sobre a temática, incluindo artigos acadêmicos, relatórios de organismos internacionais e estudos de caso que abordem a aplicação do direito da criança e do adolescente em contextos digitais.

A justificativa para a realização desta pesquisa está fundamentada na urgência de analisar os riscos crescentes associados à coleta de dados de reconhecimento facial de crianças e adolescentes, um tema pouco explorado no Brasil, mas de grande relevância no contexto da proteção dos direitos fundamentais, que podem influenciar negativamente seu desenvolvimento e bem-estar.

A estrutura do artigo é organizada da seguinte forma: na primeira parte, aborda-se a evolução das tecnologias de reconhecimento facial, com ênfase em suas implicações éticas e sociais. A seguir, analisa-se o impacto das TRFs nos direitos das crianças e adolescentes. Em continuidade, explora-se o papel do Estado na regulação dessas tecnologias, analisando legislações existentes e lacunas normativas. Por fim, realiza-se uma análise dos riscos associados ao uso dessas tecnologias nas plataformas digitais, com base na teoria dos 4Cs, propondo caminhos para mitigar os impactos negativos sobre crianças e adolescentes.

1 A EVOLUÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL: IMPLICAÇÕES ÉTICAS E SOCIAIS NO SEU USO

A tecnologia de reconhecimento facial tem avançado de forma acelerada, impulsionada por melhorias nos algoritmos de inteligência artificial e pelo aumento da capacidade de processamento de dados. Nos últimos anos, essas tecnologias passaram a integrar uma diversidade de cenários, desde o desbloqueio de dispositivos pessoais até complexos sistemas de vigilância pública.

Além das tecnologias voltadas para uso pessoal, têm sido desenvolvidas também outras aplicações das TRFs com alcance significativo, possibilitando a criação das chamadas "cidades inteligentes", interconectadas por sistemas de alta tecnologia que garantem a transmissão de informações em questão de segundos. Essa evolução acompanha a adoção de sistemas de reconhecimento facial, que são utilizados por uma variedade de motivos (Silva, Silva, 2020, p. 42).

A tecnologia de reconhecimento facial utiliza algoritmos para comparar a imagem ou vídeo de uma pessoa com um banco de dados previamente armazenado. O sistema rastreia e mapeia os padrões de uma face humana para identificar suas características únicas. Esse processo é fundamental para a identificação, pois envolve a análise detalhada de diferentes aspectos da face, como a distância entre os olhos, a forma do nariz e a estrutura da mandíbula (Kleina, 2021).

Essa tecnologia, que compara um rosto escaneado ou um material em vídeo com uma base de dados, promete um grande ganho em termos de eficiência e celeridade. O reconhecimento facial é uma ferramenta que utiliza padrões biométricos para distinguir uma pessoa com mais agilidade e precisão, assim como outras formas de identificação biométrica como as impressões digitais ou leitura

da íris, o reconhecimento facial considera características únicas de um indivíduo para confirmar que ele é quem diz ser (Boarini, 2020).

Os pontos nodais no rosto de uma pessoa são as variáveis que tornam cada ser humano único, como espaço entre os olhos, espessura dos lábios, cicatrizes, marcas de expressão, comprimento do nariz, dentre outras características. Assim, é criado um mapa facial permitindo que as tecnologias de reconhecimento façam a validação e identificação daquele indivíduo (Gryfo, 2021).

Algumas discussões podem surgir com a utilização dessa tecnologia, como taxas de erro mais altas para certos grupos demográficos, falta de privacidade dos cidadãos, risco de vazamento ou roubo dos dados e a violação do direito à proteção de dados, em especial aqueles relativos às crianças e adolescentes. Isso porque, o sistema de reconhecimento facial não pede permissão para fazer a varredura de informações. Outro lado controverso desta ferramenta é a coleta massiva de dados pessoais que, posteriormente, alimentam os algoritmos, ajudando a definir padrões de comportamento e consumo na sociedade contemporânea.

Necessário, todavia, refletir sobre como as TRFs podem ser falhas e agravar situações discriminatórias ao coletar dados e o que pode ser feito a respeito dessa questão. Exemplificando, os funcionários de uma loja nos Estados Unidos demostraram que câmeras da Hewlett-Packard (HP MediaSmart), com capacidade de identificar e seguir rostos nas imagens, funcionavam conforme o esperado com uma funcionária branca, mas eram incapazes de reconhecer o rosto de seu colega negro (Chen, 2009).

O Brasil é o quinto país que mais possui câmeras do tipo Hikvision e Dahua, conhecidas por sua alta capacidade de reconhecimento facial. Essas câmeras de vigilância são utilizadas na China e o seu uso já foi apontado como violador de direitos humanos, tendo em vista a capacidade das câmeras de perfilamento das pessoas, com base na raça ou etnia. Isso porque as TRFs utilizam inteligência artificial por meio de atividade algorítmica, algo ainda não regulado e que, muitas vezes, pode ser utilizado em desconformidade com leis e garantias fundamentais (Costa; Kremer, 2022, p. 148).

No Brasil, a pesquisa intitulada "Esporte, Dados e Direitos: O Uso de Reconhecimento Facial nos Estádios Brasileiros", desenvolvida pelo projeto Panóptico do CESeC, aborda criticamente a implementação de TRFs em estádios de futebol no Brasil. O estudo destaca como esses sistemas, inseridos no contexto da Lei Geral do Esporte e do programa Estádio Seguro, transformam espaços de lazer e cultura em locais de vigilância intensiva e coleta massiva de dados pessoais, gerando preocupações relacionadas à privacidade, direitos fundamentais e discriminação (Sousa, 2024, p. 5).

A investigação aponta que, embora a justificativa para o uso das TRFs seja a segurança pública (como a identificação de indivíduos procurados pela justiça e a redução de cambismo), há falhas estruturais significativas. Estudos prévios e relatos de campo revelam altos índices de falsos positivos, abordagens constrangedoras e práticas discriminatórias, especialmente contra grupos racializados e vulneráveis. Adicionalmente, a integração entre dados pessoais coletados por estádios e órgãos de segurança pública, com base em exceções da Lei Geral de Proteção de Dados (LGPD), expõe lacunas regulatórias e falta de transparência (Sousa, 2024, p.11).

A pesquisa contextualiza a adoção das TRFs no Brasil como parte de uma tendência global de "datificação", em que tecnologias biométricas se tornam ferramentas de controle social. Eventos esportivos internacionais, como a Copa do Mundo de 2014 e a Copa América de 2019, serviram como laboratórios para a implementação dessas práticas (Sousa, 2024, p.17). Contudo, o avanço tecnológico não é acompanhado por mecanismos robustos de accountability e proteção dos dados, resultando em possíveis violações de direitos e exclusão social.

Entre os problemas observados estão a fragmentação de dados entre diferentes empresas e instituições, a insegurança no armazenamento de informações sensíveis e a falta de clareza sobre a finalidade e os limites do uso dos dados coletados. Além disso, o relatório evidencia que crianças e adolescentes são particularmente vulneráveis, com a coleta de seus dados biométricos muitas vezes sendo realizada sem o devido cuidado com o Estatuto da Criança e do Adolescente (ECA) e a LGPD. Exemplos incluem casos em que menores de idade foram cadastrados sem o consentimento apropriado, expondo-os a riscos de uso indevido dos dados (Sousa, 2024, p. 44).

Algoritmos podem ser definidos como rotinas logicamente encadeadas. Também podem ser compreendidos como o conjunto de instruções introduzidas em uma máquina para resolver um problema bem definido (Silveira, 2016, p. 268). Por isso, quando há a captura de imagens ou vídeos para a formação do banco de dados que servirão para as TRFs é muito importante que se saiba, de fato, como esses algoritmos estão programados para funcionar.

A todo instante, compras de mercado são registradas em programas de fidelidade que servem para a construção de perfis de consumo e análises de atividade econômica, pulseiras e relógios aferem batimentos cardíacos e temperatura corporal, compondo bases de dados usadas na gestão de leitos hospitalares e na precificação de seguros de saúde, ônibus e carros particulares carregam sensores de GPS que informam sobre o fluxo do trânsito, auxiliando no trabalho de engenheiros de tráfego e atualizando aplicativos de transporte (Ceia; Duarte, 2023, p. 15).

O fato é que, mesmo quem não investe em objetos inteligentes não está completamente salvo de intrusões indevidas, pois o recolhimento e tratamento de dados pessoais é intenso, praticamente invisível e não se restringe aos equipamentos inteligentes já que as redes sociais também tem se utilizado do data mining (exploração de dados à procura de padrões consistentes) e de outras formas de tratamento de dados para otimizar ainda mais a experiência online (Silva, Silva, 2020, p. 44).

Diante do exposto, é fundamental que o desenvolvimento de inteligência artificial assegure que os modelos algorítmicos sejam projetados com padrões sólidos de segurança, transparência e responsabilidade, sempre com a intenção de que o ser humano permaneça no centro das aplicações dessas tecnologias.

2 AS TECNOLOGIAS DE RECONHECIMENTO FACIAL E O DIREITO DAS CRIANÇAS E ADOLESCENTES: PROTEÇÃO E DESAFIOS

O uso de tecnologias por crianças e adolescentes passou por uma transformação significativa ao longo dos anos. Antigamente, as interações eram predominantemente mediadas por jogos simples, muitas vezes considerados rudimentares em comparação com as opções atuais. Hoje, o mercado se especializou e oferece uma vasta gama de tecnologias, incluindo aplicativos educacionais, plataformas de aprendizado online e dispositivos interativos, que vão além do entretenimento e promovem desenvolvimento cognitivo e social. Essa evolução reflete não apenas o avanço das tecnologias, mas também uma mudança nas expectativas das novas gerações, que buscam experiências mais ricas e envolventes.

Não há dúvidas que são muitos os usos positivos das tecnologias pelas crianças e adolescentes, todavia o contato precoce com o ambiente digital necessita acompanhamento familiar, com genitores e responsáveis que precisam exercer os deveres de cuidado e de proteção que também são aplicáveis às demais experiências a serem vivenciadas pela criança. Como afirma Nascimento Júnior (2023, pg. 39) "se os pais não deixam uma criança de oito anos sozinha na praça pública conversando com estranhos, não podem entregar dispositivo eletrônico com aplicativos que permitam comunicação direta com usuários desconhecidos".

Nessa mesma linha, o uso de TRFs transformaram o modo como a sociedade tem acesso a vários serviços. Como era de se esperar, isso reverberou igualmente na vida das crianças e adolescentes que, já nascidos imersos em profundos contextos tecnológicos presentes na sua rotina, agora vivem também sob a égide da constante coleta de seus dados pessoais. O aumento do uso das TRFs é inquestionável, o que se pode perquirir é como essas tecnologias estão sendo utilizadas. A ética dessas tecnologias depende de diversos fatores, incluindo a qualidade dos algoritmos, o treinamento dos modelos de reconhecimento e a análise das questões de privacidade.

Os dados coletados pelas TRFs muitas vezes são recolhidos e utilizados sem o devido consentimento dos titulares ou de seus responsáveis, o que levanta sérias preocupações, pois essa prática vai de encontro à legislação brasileira, como está disposto no artigo 17 do Estatuto da Criança e do Adolescente (Lei 8.069/1990), que assegura que o direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais. Ao não respeitar esses direitos, as TRFs não apenas podem comprometer a privacidade desses indivíduos, mas também podem infringir normas que visam garantir a integridade das informações pessoais dessa faixa etária.

Os fundamentos que norteiam a Lei Geral de Proteção de Dados Pessoais/LGPD (Lei 13.709/2018) também precisam ser observados pelas tecnologias que lidam com dados pessoais, a saber: o respeito à privacidade, à autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, dentre outros.

As empresas de tecnologia precisam ser transparentes e explicar como aproveitam dados pessoais por meio das TRFs, particularmente dados pertencentes a crianças e adolescentes. Isso

porque, transparência, entre usuários e empresas, gera confiança. Mais ainda, ela garante que os direitos dos mais vulneráveis sejam tratados com o devido respeito. Além de explicar quais medidas de segurança estão em vigor para proteger os dados, as organizações devem fornecer informações de forma clara e simples sobre como tais informações são coletadas, armazenadas e usadas.

A complexidade do problema aumenta porque muitos responsáveis pela proteção integral, como pais e responsáveis, não reconhecem os riscos aos quais crianças e adolescentes estão expostos. Ainda porque, estes usuários, mesmo cientes de sua exposição, frequentemente são tão atraídos pelas vantagens das tecnologias que ignoram os potenciais perigos (Hermes; Sutel; Silva, 2019, p. 08).

Alguns pais inclusive compartilham frequentemente dados pessoais de seus filhos nas redes sociais, como fotos, informações sobre saúde, locais onde estudam, amizades e atividades cotidianas. Essa prática de postagens excessivas sobre a vida dos filhos ganhou uma denominação especial: *sharenting*. Além disso, cada vez é mais comum que a vida intrauterina dos bebês também seja registrada, com a publicação de imagens de ultrassonografia, informações médicas e ensaios fotográficos, muitas vezes antes mesmo do nascimento (Ferreira, 2020, p. 03).

Recentemente, a Human Rights Watch, organização internacional não governamental, realizou denúncia apontando que 170 fotos e dados pessoais de crianças e adolescentes brasileiros foram usados sem consentimento para treinar ferramentas de Inteligência Artificial. De acordo com a organização, essas imagens e dados foram extraídos de blogs pessoais e publicações no YouTube, entre os anos 1990 e 2023, e, posteriormente, foram utilizadas para o treinamento de ferramentas de inteligência artificial.

O uso dessas imagens não foi autorizado, além do fato que foi constatado que o repositório de dados também poderia expor informações confidenciais das crianças e adolescentes, como suas localizações ou dados médicos. Uma dessas fotos mostra uma menina de 2 anos com os lábios entreabertos de admiração enquanto toca os dedinhos de sua irmã recém-nascida. A legenda e as informações incorporadas na foto revelam não apenas os nomes das duas crianças, mas também o nome e a localização exata do hospital em Santa Catarina onde o bebê nasceu, há nove anos (Brasil, 2024).

Com o avanço da doutrina jurídica relativa aos direitos das crianças e adolescentes, firmou-se o entendimento de que a teoria da proteção integral, que estabelece a responsabilidade compartilhada entre Estado, família e sociedade para garantir os direitos fundamentais desses grupos, é a mais adequada para tratar da proteção dos direitos das crianças e adolescentes.

Apesar disso, conforme Rosane Leal da Silva (2020, p. 242), o princípio do melhor interesse ainda não é adequadamente compreendido por parte dos Estados, tampouco pela família e sociedade, destinatários do comando constitucional do art. 227 que impõe a todos os atores o dever de promover a proteção integral das crianças e adolescentes. O que se percebe, com tanta exposição, é uma nova forma de objetificação de crianças e adolescentes, como se ainda se vivesse sob o paradigma do menorismo, que se manteve no Brasil até o advento da Constituição Federal de 1988.

O reconhecimento da criança e do adolescente como protagonista de seus direitos implica não apenas na defesa de sua integridade, mas também no reconhecimento de sua voz e participação em assuntos que a afetam. Essa mudança de paradigma, introduzida com a Constituição Federal de 1988 reflete um avanço no entendimento jurídico, onde o protagonismo das crianças e adolescentes se torna uma condição essencial para a efetivação dos direitos fundamentais. Contudo, apesar dos avanços normativos, a implementação prática desses direitos ainda enfrenta desafios significativos, especialmente no ambiente digital em que a figura do intermediário tradicional é substituída por plataformas digitais, que oferecem tanto liberdade quanto riscos.

Esse pensamento em relação à infância é corroborado por Manuel Jacinto Sarmento (2005) quando trata essa fase da vida a partir de uma abordagem sociológica, na qual as crianças são participantes ativos na construção da sociedade, e não apenas indivíduos em formação. Dessa forma, para o autor, a infância em vez de ser tida apenas como uma fase de maturação biológica ou psicológica, deve ser vista sob o aspecto sociológico, teoria que reconhece as crianças como atores sociais, inseridos em diferentes sociedades, o que os torna sujeitos com direito a uma investigação própria.

3 O PAPEL DO ESTADO NA REGULAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL E A LEGISLAÇÃO EM VIGOR

Nesse aspecto, o papel do Estado é crucial em regular e supervisionar o uso de tecnologias de reconhecimento. Tal atuação deve garantir que sejam utilizadas dentro do ordenamento jurídico interno de cada país, assim como trabalhar na proteção de direitos fundamentais como privacidade e proteção aos dados e, por fim, assegurar a devida transparência na utilização dos dados coletados por essas tecnologias.

Como esse setor praticamente não tem regulação, as empresas e os governos, aos poucos, estão implementando políticas e fazendo exigências maiores para utilização dessa tecnologia, mas tudo ainda é embrionário. Nesse sentido, é importante destacar que as empresas atuantes em nível transnacional ou até global se esforçam muitas vezes para subtrair-se às vinculações legais. São muitas as tentativas de driblar a vinculação jurídica, seja por meio de uma escolha deliberada da sede ou mesmo da transferência de atividades para outras partes da corporação.

No Brasil ainda não há legislação que trate desse tema específico, entretanto, recentemente foi aprovado, na União Europeia, o Regulamento específico que trata do uso das Inteligências Artificiais. As disposições desse documento proíbem explicitamente certas aplicações de Inteligência Artificial que violem os direitos dos cidadãos.

Entre essas proibições, destacam-se sistemas de categorização biométrica baseados em características sensíveis, assim como a coleta indiscriminada de imagens faciais da internet ou de gravações de câmeras de vigilância para a criação de bancos de dados de reconhecimento facial. São vedadas, igualmente, práticas como o reconhecimento de emoções no ambiente de trabalho e em

escolas, sistemas de pontuação cidadã, policiamento preditivo e IA que manipula o comportamento humano ou explora vulnerabilidades (Alcassa, 2024).

Apesar de não haver lei promulgada sobre o tema, existem iniciativas legislativas brasileiras, como o Projeto de Lei 2.338/23, que trata do emprego de IA. Este projeto tem como objetivo regulamentar aspectos pertinentes ao uso dessas tecnologias em território nacional, com o objetivo de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico (Brasil, 2023). O Senado Federal aprovou, no dia 10 de dezembro de 2024, um projeto de lei com texto substitutivo, que teve como base o PL 2338/23, e que agora segue para análise na Câmara dos Deputados.

A busca por delinear traços comuns humanos para antecipar comportamentos não é nova, pois Cesare Lombroso, por exemplo, ao estudar traços faciais e compleições corporais, procurou estabelecer uma ligação entre essas características com as tendências criminosas dos delinquentes. No entanto, a tecnologia referente a essa temática começou a ser desenvolvida de forma mais expressiva na década de 90, quando o avanço na capacidade de processamento e a disponibilização de amplas bases de dados para treinamento dos algoritmos levaram ao ganho de precisão e à redução de custos.

As TRFs atuais funcionam a partir de alguns passos específicos. Inicialmente, imagens são capturadas por instituições públicas ou privadas (como forças policiais, departamentos de trânsito, agências de identificação civil, empresas privadas de segurança, bancos etc.). Em seguida, essas imagens são convertidas em códigos alfanuméricos, que passam então a integrar as bases com as quais serão feitas as análises.

Na fase operacional, uma nova imagem é capturada e comparada com o arquivo para verificação de identidade. O resultado do sistema algorítmico não é uma resposta definitiva (sim ou não), mas um cálculo de probabilidade que atesta qual é a chance da nova imagem ser correspondente à pessoa cujo dado biométrico estava no arquivo (Tecnologia, Segurança e Direitos, 2023, p. 18).

Dessa forma, o reconhecimento facial pode significar uma violação inerente ao tratamento de dados biométricos. Segundo o art. 5º, II da Lei Geral de Proteção de Dados Pessoais, esses dados são considerados sensíveis, ou seja, dados que, quando tratados de forma inadequada ou irregular, podem causar ou intensificar contextos discriminatórios para os titulares, podendo resultar em danos à personalidade.

A LGPD prevê a categoria de dados sensíveis como forma de garantir uma maior proteção diante de formas de tratamento potencialmente discriminatória e lesiva. O art. 5º, II, da LGPD define como sensíveis os dados pessoais sobre raça, etnia, religião, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Ainda sob o viés da necessidade de especial proteção aos dados de crianças e adolescentes, em junho do presente ano foi apresentado o Projeto de Lei nº 2416/2024, que visa regulamentar o uso

de tecnologias de vigilância. O projeto define como tecnologias de vigilância “qualquer software, hardware ou serviço utilizado para monitorar, registrar, coletar ou analisar dados pessoais ou comportamentais de indivíduos” (Internetlab, 2024). O PL veda o uso dessas tecnologias para a coleta de dados pessoais de crianças e adolescentes sem o consentimento dos responsáveis legais.

Portanto, permanece o questionamento de como, na prática, deveria ocorrer a coleta dos dados de crianças e adolescentes com o uso das TRFs, uma vez que a Constituição Federal e o Estatuto da Criança e do Adolescente conferem proteção integral a esses indivíduos através de vários mecanismos jurídicos, a serem implementados em sistema de responsabilidade compartilhada pela família, sociedade e Estado (Silva, 2009, p. 20).

A evolução dos direitos das crianças e adolescentes é um marco fundamental na construção da sociedade contemporânea. Desde a Declaração dos Direitos da Criança, em 1959, até a adoção da Convenção sobre os Direitos da Criança, em 1989, a compreensão da infância passou por transformações significativas. Esses documentos internacionais estabeleceram uma nova perspectiva sobre a criança, não mais como alguém a ser protegido passivamente, mas como um sujeito ativo, detentor de direitos e que deve ter reconhecido o seu poder de agência.

3.1 RECONHECIMENTO FACIAL E OS RISCOS NAS REDES SOCIAIS: O CASO DO TIKTOK

As redes sociais se utilizam de inteligência artificial, com algoritmos cada vez mais sofisticados e capazes de recolher e tratar dados pessoais. Dentre essas redes que se notabilizam pelo uso dessas tecnologias encontra-se a Plataforma TikTOk.

A popularização do TikTok entre crianças e adolescentes expõe uma série de desafios regulatórios e jurídicos que orbitam o uso de tecnologias baseadas em reconhecimento facial. Apesar de os Termos de Serviço (TikTok, 2024) da plataforma indicarem uma idade mínima de 13 anos para utilização, a realidade cotidiana revela a massiva presença de usuários muito abaixo dessa faixa etária, muitos dos quais têm livre acesso ao aplicativo sem qualquer verificação robusta de idade. Isso expõe diretamente essa população vulnerável aos sistemas de coleta de dados biométricos e algoritmos opacos, cujas finalidades e desdobramentos nem sempre são claros.

Mais do que uma questão técnica ou contratual, identifica-se uma problemática que envolve o direito fundamental à proteção dos dados pessoais de crianças e adolescentes, que se revestem de caráter especial. Ciente disso, o Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA), editou a Resolução nº 245, de 5 de abril de 2024, que classifica expressamente os dados de crianças e adolescentes como dados pessoais sensíveis, exigindo, portanto, um nível máximo de proteção e tratamento responsável. Ademais, esta Resolução orienta que as plataformas digitais devem implementar mecanismos eficazes para mitigar riscos de vigilância, *profiling*, exploração econômica e discriminação algorítmica.

Esse tipo de vigilância silenciosa transforma a experiência online da criança em um objeto de mercantilização, sem que haja uma real possibilidade de escolha ou compreensão sobre os efeitos

dessa coleta contínua. A Resolução nº 245/2024 do Conanda dispõe que empresas devem adotar "mecanismos de verificação de idade e consentimento de forma clara, objetiva e acessível". No entanto, o TikTok, embora mencione o limite etário de 13 anos, não implementa medidas robustas de verificação, permitindo que menores de idade acessem a plataforma com facilidade. Esse descumprimento não é apenas uma falha técnica, mas uma violação direta ao princípio do melhor interesse da criança, constitucionalmente garantido no Brasil e destacado no art. 14, da LGPD.

A naturalização da presença de crianças em ambientes digitais, como o TikTok, mascara uma profunda assimetria de poder entre os usuários infantis e as corporações tecnológicas. Crianças não são apenas usuárias, mas sim, sobretudo, alvos de coleta de dados em grande escala. Tanto é evidente sua vulnerabilidade, em escala global, que o Comitê sobre os Direitos da Criança, da ONU editou, em 2021, o Comentário Geral nº 25. Este importante documento internacional alerta que o uso de tecnologias digitais deve ser sempre compatível com o desenvolvimento integral da criança, com especial atenção à sua privacidade, liberdade de expressão e proteção contra abusos (ONU, 2021). Ao reconhecer essa vulnerabilidade, o documento reforça as responsabilidades das empresas que atuam no segmento, que devem "avaliar proativamente os impactos de suas tecnologias sobre os direitos das crianças", inclusive antes da implementação de novos recursos.

Não obstante esses deveres, elencados no documento, o TikTok opera com modelos de negócio centrados em extração de dados, o que fere diretamente o princípio da autodeterminação informacional, consagrado pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), especialmente em relação a dados sensíveis. A plataforma não disponibiliza ferramentas adequadas para que pais ou responsáveis possam exercer controle efetivo sobre os dados dos menores de idade, o que resulta numa invisibilização da tutela parental no ambiente digital.

Ainda mais preocupante é o fato de que o TikTok utiliza tecnologias de detecção facial para classificar rostos, identificar traços e expressões, e assim inferir emoções e estados mentais. Essa prática se insere na lógica do "capitalismo de vigilância" (Zuboff, 2020), em que até o afeto se torna um ativo digital mensurável e comercializável. Para crianças, isso representa uma forma precoce de alienação subjetiva, já que suas emoções e comportamentos passam a ser moldados em função de estímulos projetados para maximizar engajamento, visualizações e lucro.

Em sintonia com o Comentário n. 25 e para implementá-lo, o Ministério da Justiça e Segurança, brasileiro, editou a Portaria Interministerial nº 12/2023, reforçando que plataformas digitais devem redigir termos de uso em linguagem acessível para o público infantojuvenil, permitindo a compreensão clara dos riscos envolvidos (Brasil, 2023). Todavia, ao observar os Termos de Serviço do TikTok, percebe-se que os documentos permanecem com linguagem técnica, vaga e de difícil compreensão até mesmo para adultos, quiçá para crianças. Tal opacidade impede o exercício do consentimento informado e viola o direito à informação, previsto no Estatuto da Criança e do Adolescente.

Na mesma linha do documento lançado pelo Ministério da Justiça e Segurança, a Secretaria de Comunicação Social do Governo Federal produziu o Guia "Direitos Digitais de Crianças e Adolescentes", no qual se estabelece como dever das plataformas "adotar políticas de moderação de

conteúdo e de design centrado na criança" (Brasil, 2023). O TikTok, no entanto, não apresenta mecanismos suficientes de moderação humanizada que evitem a exposição de menores de idade a desafios perigosos, conteúdos sexualizados ou estímulos que incentivam transtornos alimentares e comportamentos autodestrutivos, situações amplamente documentadas por especialistas em infância e juventude.

Em uma sociedade digital que se constrói com base no consumo de atenção, a exposição continuada de crianças a ambientes altamente gamificados como o TikTok pode contribuir para a formação de padrões cognitivos e afetivos pautados na recompensa instantânea, prejudicando o desenvolvimento da atenção sustentada, da empatia e da resiliência emocional.

A ausência de um controle social mais efetivo sobre essas práticas corporativas demonstra o descompasso entre o avanço tecnológico e a garantia de direitos fundamentais. A regulação da inteligência artificial, quando aplicada ao reconhecimento facial, deve priorizar os sujeitos mais vulneráveis, como é o caso de crianças e adolescentes. Isso significa impor limites, criar salvaguardas jurídicas, promover a fiscalização contínua e exigir que plataformas, como o TikTok, prestem contas de forma transparente à sociedade civil e aos órgãos de proteção da infância.

4 ANÁLISE DOS RISCOS NAS PLATAFORMAS DIGITAIS E A CLASSIFICAÇÃO DOS 4CS

Para tentar compreender esse cenário digital peculiar que envolve as crianças e os adolescentes utilizou-se a teoria dos 4Cs (Conteúdo, Contato, Conduta e Contrato) desenvolvida por Sonia Livingstone e Mariya Stoilova (2021), que oferece uma estrutura conceitual para analisar os riscos que crianças e adolescentes enfrentam no ambiente digital. Essa abordagem permite a possibilidade de mapear os diferentes tipos de riscos digitais e compreender como eles afetam, de maneira aprofundada, os direitos das crianças.

A escolha desse modelo para explorar a relação entre as TRFs e a proteção de dados de crianças e adolescentes fundamenta-se na sua capacidade de distinguir e desagregar os riscos em categorias específicas. A integração das TRFs no ambiente digital amplia a exposição das crianças a riscos contratuais, como o uso indevido de seus dados biométricos, e reforça a necessidade de investigar como esses dados são coletados, armazenados, utilizados e, posteriormente, compartilhados.

A classificação dos 4Cs surgiu como uma evolução do modelo anterior dos 3Cs, uma vez que incluiu "Contrato" como uma nova dimensão crítica. Essa inclusão reflete as mudanças no ecossistema digital e as novas formas de exploração comercial e coleta de dados envolvendo crianças (Livingstone; Stoloiva, 2021. p. 3).

O modelo busca desagregar os riscos enfrentados pelas crianças ao explorar sua posição como usuárias ativas, vítimas ou testemunhas no ambiente digital. Além disso, ele aborda a interação entre esses riscos e os aspectos psicológicos, sociais e tecnológicos que os potencializam (Livingstone; Stoloiva, 2021. p. 4). A sistematização oferecida pelos 4Cs é essencial para o

desenvolvimento de políticas públicas, regulamentações e estratégias educacionais que visem proteger os direitos das crianças e adolescentes, de modo que seja possível aumentar o nível de segurança em relação ao ambiente digital (Nascimento Júnior, 2024. p 84).

Em um cenário tecnológico em constante transformação, a clareza conceitual proporcionada por essa estrutura auxilia na formulação de políticas públicas, práticas educacionais e mecanismos regulatórios que busquem garantir um ambiente digital mais seguro. O modelo também oferece um referencial prático para que pais, educadores e legisladores compreendam os tipos de riscos e as dinâmicas envolvidas nas interações digitais das crianças, possibilitando ações preventivas e corretivas com maior precisão (Livingstone; Stoloiva, 2021. p. 12).

Essa abordagem destaca-se ainda por considerar a criança como um indivíduo com agência no ambiente digital, mas que, ao mesmo tempo, necessita de proteção diante de fatores que ultrapassam sua capacidade de controle ou compreensão. Isso envolve desde a exposição a conteúdos inadequados até interações prejudiciais e riscos decorrentes de práticas comerciais exploratórias. A classificação, portanto, promove um equilíbrio entre a proteção da criança e o respeito ao seu direito de acesso às oportunidades digitais, alinhando-se às discussões contemporâneas sobre direitos fundamentais no ambiente online (Nascimento Júnior, 2024. p. 293).

Esse modelo foi utilizado por pesquisadores e organizações internacionais em análises de risco e em debates sobre segurança digital infantil, pois sua flexibilidade permite adaptação às especificidades de diferentes contextos socioculturais, o que o torna uma ferramenta valiosa para mapear os desafios enfrentados pelas crianças em realidades distintas, como a exposição às tecnologias de reconhecimento facial tratadas no presente estudo. Além disso, tem contribuído para uma abordagem mais colaborativa na promoção de um ambiente digital mais ético e inclusivo (Nascimento Júnior, 2024. p.269), como se verá na sequência.

4.1 Classificação dos 4Cs (Conteúdo, Contato, Conduta e Contrato) como Ferramenta de Análise

O primeiro "C", Conteúdo, refere-se aos riscos decorrentes da exposição a materiais inadequados ou potencialmente prejudiciais. As crianças podem acessar conteúdos violentos, odiosos, pornográficos ou extremistas, que impactam negativamente seu desenvolvimento emocional, cognitivo e social. A internet permite tanto a produção em massa por grandes empresas quanto a criação de conteúdo gerado por usuários, tornando o controle mais desafiador (Livingstone; Stoloiva, 2021. p.6).

A situação pode ser agravada, uma vez que os algoritmos podem alimentar perfis automatizados das crianças e sugerir conteúdos inadequados com base em suas interações digitais. Em acréscimo, há o risco de normalização de temas impróprios, uma vez que os sistemas automatizados nem sempre conseguem distinguir o que é apropriado para cada faixa etária.

O segundo "C", Conduta, trata dos riscos relacionados às ações de crianças no ambiente digital, como participar, testemunhar ou ser vítima de comportamentos prejudiciais. Exemplos

incluem *bullying*, assédio, *trolling* e exposição a comunidades perigosas que incentivam práticas nocivas, como automutilação ou transtornos alimentares. O ambiente digital potencializa essas interações, muitas vezes removendo barreiras físicas e sociais que poderiam servir como limites no mundo *offline* (Livingstone; Stoloiva, 2021. p.6).

Essas práticas podem ser muito problemáticas, pois os dados biométricos coletados através das tecnologias de reconhecimento facial podem ser usados para rastrear comportamentos e ações *online*, violando direitos de privacidade e expondo as crianças e adolescentes a consequências imprevisíveis.

O terceiro "C", Contato, aborda os riscos relacionados às interações que as crianças têm com adultos mal-intencionados no ambiente digital. Essas interações podem incluir aliciamento sexual, sextorsão, assédio ou outras formas de exploração (Livingstone; Stoloiva, 2021. p.6).

As TRFs podem elevar esses riscos ao permitir que adultos, muitas vezes desconhecidos, utilizem informações coletadas para rastrear ou identificar crianças de maneira mais precisa. A ausência de regulamentação clara sobre o uso de dados biométricos, especialmente de crianças, agrava a situação, pois os próprios sistemas podem facilitar o acesso indevido a informações sensíveis.

O quarto "C", Contrato, reflete os riscos comerciais enfrentados pelas crianças no ambiente digital. Este último elemento foi incluído mais recentemente no modelo, reconhecendo a crescente exploração comercial e coleta de dados no ecossistema digital. Crianças podem ser alvo de práticas como marketing exploratório, contratos desleais ou inseguros, e até mesmo fraudes e roubo de identidade (Livingstone; Stoloiva, 2021. p.6).

O problema se torna ainda mais grave quando crianças são exploradas comercialmente sem o devido consentimento ou mesmo sem o conhecimento de seus responsáveis. Casos de "*sharenting*", em que pais compartilham dados e imagens de seus filhos *online*, também exemplificam como práticas aparentemente inofensivas podem levar à exploração de crianças em contextos comerciais.

No atual contexto tecnológico, onde o digital permeia todos os aspectos da vida das crianças, essa classificação é uma ferramenta didática que pode nortear políticas públicas, práticas educacionais e ações preventivas voltadas à proteção da infância e adolescência. A classificação também pode ser útil por destacar a necessidade de equilibrar a proteção com a promoção do protagonismo digital das crianças, permitindo que elas tenham acesso às oportunidades tecnológicas de forma segura e informada.

CONCLUSÃO

A crescente inserção de crianças e adolescentes no ambiente digital, aliada à expansão das tecnologias de reconhecimento facial, apresenta um grande desafio, pois ao mesmo tempo que oferecem avanços significativos, também podem ampliar os riscos à privacidade, autonomia e dignidade dos sujeitos mais vulneráveis da sociedade.

Neste contexto, a análise apresentada neste artigo evidencia que a lacuna regulatória no Brasil, combinada à insuficiente conscientização de famílias e da sociedade em geral, contribui para a perpetuação de práticas que podem comprometer os direitos fundamentais de crianças e adolescentes. A tecnologia de reconhecimento facial certamente é um grande progresso no campo da inteligência artificial. Contudo, quando aplicada de maneira indiscriminada e sem diretrizes claras, pode se transformar em uma ameaça ao direito à privacidade e à proteção dos dados de crianças e adolescentes.

A legislação brasileira, embora conte com marcos importantes como o ECA e a LGPD, ainda não oferece mecanismos suficientemente específicos para regular o uso de tecnologias emergentes. Em particular, a falta de diretrizes claras sobre o consentimento para a coleta de dados biométricos, especialmente no caso de crianças e adolescentes, é preocupante. Exemplos práticos, como o uso de reconhecimento facial em escolas para monitorar a presença de alunos, mostram que muitas vezes esses dados podem estar sendo coletados sem o devido consentimento informado dos responsáveis, em clara violação às normas legais vigentes. Essa preocupação se amplia diante de termos de uso como os da plataforma TikTok, que preveem a coleta de identificadores faciais e de voz, agravando a necessidade de regulação efetiva e fiscalização específica.

A aplicação da teoria dos 4Cs é uma direção possível para entender os riscos associados ao uso das TRFs em relação à proteção de dados de crianças e adolescentes. Com ela, torna-se possível mapear as diferentes ameaças às quais crianças e adolescentes podem estar expostos, auxiliando a expor aspectos que vão desde a coleta inicial dos dados até o impacto social e psicológico do uso dessas tecnologias, evidenciando a complexidade do problema.

Ao propor uma análise estruturada, os 4Cs possibilitam caminhos para compatibilizar o avanço dessa tecnologia com os direitos fundamentais dos menores de idade. Essa integração de perspectivas de risco e oportunidades não apenas reconhece o possível potencial positivo ou negativo das TRFs, mas, sobretudo, sublinha a necessidade de garantir que elas sejam utilizadas em conformidade com os princípios de segurança, privacidade e dignidade, resguardando o bem-estar das crianças no ambiente digital.

A classificação dos 4Cs mostra-se uma ferramenta útil para identificar e traçar caminhos para mitigar riscos no ambiente digital. No entanto, sua aplicação no contexto das tecnologias de reconhecimento facial exige adaptações que considerem as especificidades desses sistemas. Por exemplo, o "C" de Conteúdo precisa incorporar discussões sobre o impacto de algoritmos que podem sugerir materiais inapropriados com base em perfis automatizados, enquanto o "C" de Contato deve incluir os riscos de rastreamento e identificação indevida possibilitados por essas tecnologias.

Sob o prisma da ética, o uso de tecnologias de reconhecimento facial coloca em debate a capacidade das empresas de tecnologia de respeitar princípios fundamentais, como transparência, equidade e *accountability*. A falta de explicações claras sobre como os dados biométricos de crianças são coletados, armazenados e utilizados não apenas compromete a confiança entre usuários e empresas, mas também dificulta a responsabilização em casos de abuso. Além disso, há o risco de discriminação algorítmica, em que falhas nos modelos de inteligência artificial podem exacerbar

preconceitos existentes, impactando negativamente grupos vulneráveis, como crianças de minorias étnicas.

Nesse contexto, o papel do Estado é indispensável. Regulamentações que estabeleçam padrões mínimos para o uso ético e responsável de tecnologias de reconhecimento facial são urgentes. Projetos de lei em tramitação, como o PL nº 2338/2023, oferecem perspectivas promissoras, mas ainda precisam ser aprovados e promulgados para que façam parte do ordenamento jurídico brasileiro. Contudo, mais do que legislar, o Estado deve assumir uma postura ativa na fiscalização, garantindo que as diretrizes legais sejam efetivamente aplicadas e que os infratores sejam responsabilizados.

A família e a sociedade, por sua vez, precisam reconhecer sua parcela de responsabilidade na proteção dos direitos de crianças e adolescentes. Práticas como o sharenting (compartilhamento excessivo de informações e imagens de crianças por seus responsáveis nas redes sociais) expõem esses sujeitos a riscos que vão desde a exploração comercial até o roubo de identidade. De forma mais próxima, os genitores/responsáveis devem ser capacitados para compreender os perigos associados às tecnologias digitais, para que possam promover um uso responsável e consciente dessas ferramentas.

A proteção integral, princípio norteador do ECA, ganha uma nova dimensão na era digital. Mais do que nunca, é preciso reforçar que o dever de proteger as crianças e adolescentes recai sobre o Estado, a família e a sociedade em geral. É essencial reconhecer que o avanço tecnológico não pode ser feito às custas de direitos fundamentais das crianças e adolescentes. O uso de tecnologias de reconhecimento facial deve ser subordinado a valores éticos que coloquem o ser humano no centro das decisões, considerando-se todos os riscos a que podem estar expostos.

REFERÊNCIAS

ALCASSA, Flávia. **Aprovação da lei da inteligência artificial na União Europeia e os desafios no Brasil**. Migalhas. Cidade. 15/04/2024. Disponível em: https://www.migalhas.com.br/depeso/405358/aprovacao-da-lei-da-inteligencia-artificial-na-ue-e-desafios-no-brasil/. Acesso em 03/12/2024.

BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA). **Resolução nº 245, de 5 de abril de 2024**. Disponível em: file:///C:/Users/camil/Downloads/resoluCAo-n-245-de-5-de-abril-de-2024-resoluCAo-n-245-de-5-de-abril-de-2024-dou-imprensa-nacional.pdf. Acesso em: 08 abr. 2025.

BRASIL. Secretaria de Comunicação Social da Presidência da República. **Direitos digitais de crianças e adolescentes**. Brasília, 2023. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/capitulos/direitos-digitais-de-criancas-e-adolescentes. Acesso em: 08 abr. 2025.

BRASIL. Senado Federal. **PL 2338/2023** -. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 19 jul. 2024.

BRASIL: Fotos de crianças são usadas indevidamente para alimentar IA. Human Rights Watch, 10/06/2024. Disponível em: https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools. Acesso em: 03/12/2024.

BOARINI, Julia. **O que é reconhecimento facial?** Veja como a tecnologia funciona. Blog Idwall. Cidade. 25/09/2020. Disponível em: https://blog.idwall.co/o-que-e-reconhecimento-facial/. Acesso em 03/12/2024.

CEIA, Eleonora; DUARTE, Daniel. **Tecnologia, Segurança e Direitos**: Os usos e riscos de sistemas de reconhecimento facial no Brasil. In: CEIA, Eleonora; DUARTE, Daniel (Org.). Introdução. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 15-32.

CHEN, B. "**HP Investigates Claims of 'Racist' Computers**". Wired, 22 de dezembro de 2009. Disponível em: https://www.wired.com/2009/12/hp-notebooks-racist/. Acesso em 16 jul. 2024.

Costa, R. S., & Kremer, B. (2022). **Inteligência artificial e discriminação**: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira De Direitos Fundamentais & Justiça, 16(1). https://doi.org/10.30899/dfj.v16i1.1316

DIAS, Felipe da Veiga. **O direito à informação na infância online**. Curitiba: Editora Prismas, 2016. Disponível em: https://repositorio.unisc.br/jspui/bitstream/11624/473/1/Felipe%20da%20Veiga%20Dias.pdf.

DIAS, Vanina Costa et al. **Adolescentes na Rede**: Riscos ou Ritos de Passagem? Psicol. cienc. prof., Brasília, v. 39, e179048, 2019. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1414-98932019000100109&lng=en&nrm=iso. Access on: 23 Nov. 2020. Epub Apr 25, 2019. https://doi.org/10.1590/1982-3703003179048.

Esporte, dados e direitos [livro eletrônico]: o uso de reconhecimento facial nos estádios brasileiros / Raquel Sousa...[et al.]; edição Marília Gonçalves. – Rio de Janeiro: CESeC, 2024.

FERREIRA, Hugo Monteiro; FERREIRA, Fernando Ilídio; MELO, Bruno Cézar de Férias. **A adultização infantil na contemporaneidade**: as escolhas das crianças. Revista Humanidades e Inovações, v. 8, n. 68, 2021. Disponível em: https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/7040. Acesso em: 15 mai. 2022.

FERREIRA, Lucia Maria Teixeira. **A superexposição dos dados e da imagem de crianças e adolescentes na Internet e a prática de Sharenting**: reflexões iniciais. Revista do Ministério Público do Estado do Rio de Janeiro, nº 78, p. 165-183, out./dez. 2020.

GRYFO. **Sistema de reconhecimento facial: boas práticas**. Disponível em: <https://gryfo.com.br/blog/2021/04/12/boas-praticas-sistema-de-reconhecimento-facial/>. Acesso em: 22 jul. 2024.

HAMILL, J. "**Chinese iPhone X owners claim Apple's Face ID facial recognition cannot tell them apart**". Metro, 22 de dezembro de 2018. Disponível em: https://metro.co.uk/2017/12/22/iphone-x-racist-cant-tell-chinese-people-apart-apple-customersclaim-7178957/. Acesso em 16 jul. 2024.

HERMES, Pedro Henrique; SUTEL, Roberta de Oliveira. SILVA, Rosane Leal da. A vigilância dos dados pessoais de crianças e adolescen**tes frente à lei geral de proteção de dados pessoais e a doutrina da proteção integral**. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/11.5.pdf. Acesso em 23 jul. 2024.

INTERNETLAB. **Projeto busca regulamentar uso de tecnologias de vigilância**. Disponível em: https://internetlab.org.br/pt/semanario/21-06-2024/. Acesso em: 22 jul. 2024.

KLEINA, Nilton. **Como funcionam os sistemas de reconhecimento facial**. Tecmundo, 24 mar. 2021. Disponível em: https://www.tecmundo.com.br/camera-digital/10347-como-funcionam-os-sistemas-de-reconhecimento-facial.htm. Acesso em: 9 dez. 2024.

LIVINGSTONE, Sonia; MASCHERONI, Giovanna; STAKSRUD, Elisabeth. **European research on children's internet use**: assessing the past and anticipating the future. New Media & Society, v. 20, n. 3, p. 1103-1122, 2018. Disponível em: http://eprints.lse.ac.uk/68516/. DOI: 10.1177/1461444816685930. Acesso em: 03/12/2024.

LIVINGSTONE, Sonia; STOILOVA, Mariya. **The 4Cs**: Classifying Online Risk to Children. Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence, 2021. Disponível em: https://doi.org/10.21241/ssoar.71817. Acesso em: 03/12/2024.

NASCIMENTO JÚNIOR, Moacir Silva do. **Crianças no ambiente digital**: riscos, oportunidades e repressão a ilícitos do mercado de atenção. 2024. Tese Doutorado em Direito. Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Comitê sobre os Direitos da Criança. **Comentário Geral nº 25 (2021) sobre os direitos das crianças em relação ao ambiente digital.** 2021. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2022/01/comentario-geral-n-25-2021.pdf. Acesso em: 08 abr. 2025.

SARMENTO, Manuel Jacinto. **Gerações e alteridade**: interrogações a partir da sociologia da infância. Educ. Soc., Campinas, v. 26, n. 91, p. 361-378, Aug. 2005. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-73302005000200003&lng=en&nrm=iso. Access on: 31 July 2019.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. **Infância vigiada**: o reconhecimento facial de crianças e adolescentes e os riscos de violação de dados pessoais. In: VERONESE, Josiane Rose Petry. Estatuto da Criança e do Adolescente: 30 anos, grandes temas, grandes desafios. p. 41-66.

SILVA, Rosane Leal da. **A proteção integral dos adolescentes internautas**: limites e possibilidades em face dos riscos no ciberespaço. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito pela Universidade Federal de Santa Catarina, Florianópolis, 2009.

SILVA, Rosane Leal da. **O tratamento de dados pessoais de crianças e adolescentes pelo Poder Público**: entre violação e proteção. In: LIMA, Cíntia Rosa Pereira de. Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, 2020, p. 225-248.

SILVEIRA, Sergio Amadeu. **Governos dos Algoritmos**. Disponível em: https://periodicoseletronicos.ufma.br/index.php/rppublica/article/view/6123/4492. Acesso em: 15 de julho de 2024.

Tecnologia, Segurança e Direitos: Os usos e riscos de sistemas de reconhecimento facial no Brasil/organização Daniel Edler Duarte e Eleonora Mesquita Ceia. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (pdf). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

TV BAHIA. **"Escola municipal de Mata de São João, na BA, usa reconhecimento facial para controlar presença de alunos"**. Disponível em: https://g1.globo.com/ba/bahia/noticia/2022/02/07/escola-municipal-de-cidadeda-ba-usareconhecimento-facial-para-controlar-presenca-de-alunos.ghtml. Acesso em: 23 mar. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.